

REMARKS

Reconsideration of the present application is respectfully requested. Claims 1-5, 9, 10 and 13 have been amended. Claims 42-71 have been newly added. Claims 16-41 have been canceled. No new matter has been added.

Claim Rejections

Independent claim 1 stands rejected under 35 U.S.C. § 103(a) based on Garrison (U.S. Patent no. 6,275,939) in view of Ji (U.S. Patent no. 5,623,600). Applicant respectfully traverses the rejections.

The present invention relates to a method of using a cluster device (a personal computer, for example) to perform an operation on an object maintained at a server (a file server, for example) upon a request to access the object by a client. The operation performed on the object may include, for example, scanning the object for virus detection. Based on the scan result, the server determines whether the access request from the client should be allowed. Because server devices are often very specialized, specialized scanning software often needed to be developed for them. The present invention is advantageous by using a less specialized cluster device to do the scanning work, avoiding the cost to develop and maintain specialized scanning software for the server.

Claim 1 recites:

1. (Currently amended) A method including
receiving a user request for **an object maintained at a server;**
upon a request from the server, performing an operation on data associated with said object at a cluster device, said cluster device being a separate device from said server, said operation including accessing said object and determining a result of scanning said object at said cluster device; and

conditionally allowing access to said object in response to said user request based on said result.
(emphasis added)

Applicant appreciates the Examiner's acknowledgement that Garrison does not teach or suggest an object and an operation including determining a result of scanning an object at a cluster device (*see* final office action mailed on 2/23/06, page 3), but further points out that Garrison and Ji, individually or in combination, also do not teach or suggest the above emphasized limitations of claim 1.

Garrison discloses a server system which allows a client to remotely access a database yet the client does not need to conform to the protocol used by the database. Assuming *arguendo* the server system, the database, or the combination of the two constitute a server such as recited in claim 1 (hereinafter the "server"), no matter which one does, Garrison still does not teach or suggest the above emphasized limitation (in bold). For example, assuming *arguendo* that the database constitutes the "server", the database just simply returns data requested by the server system (on behalf of a client). The database issues no request to the server system or any other device to perform a scan operation on the data. On the other hand, assuming *arguendo* the server system in Garrison constitutes the "server", then the requested data (or object) is not maintained at the "server" of claim 1, but at the database. Assuming *arguendo* the combination of the server system and the database constitutes the "server" as recited in claim 1, then there is no separate cluster device for performing an operation on data maintained at the "server". Therefore, whatever the interpretation may be, Garrison does not teach or suggest the above emphasized limitations in claim 1, namely, upon a request from the server, performing an operation on data associated with said object at a cluster device, said cluster device being a

separate device from said server, said operation including accessing said object and determining a result of scanning said object at said cluster device.

Neither does Ji teach or suggest the above emphasized limitations of claim 1. Ji discloses an intermediate system residing between two networks. The intermediate system scans every data packet (a file, for example) transmitted between the two networks. Specifically, the intermediate system may be a gateway holding FTP servers for transmitting files between a client and a server (*see* Ji's figures 5A and 5B). Although the gateway performs a virus scan on any file stored on a server and requested by a client, the gateway does not perform the scan upon a request from the server to perform the scan. Assuming *arguendo* that the gateway constitutes the "server", then the scan operation is performed on the "server" (*see* Ji's column 8 line 65 – column 9 line 3), not a cluster device separate from the "server", such as recited in claim 1.

Further, as discussed above, the present invention is advantageous by using less specialized cluster device to do the scanning work, avoiding the cost and need to develop and maintain specialized scanning software for the server. By contrast, neither Ji nor Garrison have suggestion or indication of the desirability of the present invention. Thus, claim 1 is not obvious in view of Ji, Garrison, or the combination of them.

At least for the above reasons, the Examiner fails to make a *prima facie* case of obviousness under §103(a). Thus, claim 1 and all claims which depend on it are patentable over Garrison and Ji.


The newly added independent claims 42 and 57 contain similar limitations as discussed for claim 1. Therefore, for similar reasons, claims 42, 57 and all claims which depend on them are also patentable over Garrison and Ji.

For the foregoing reasons, the present application is believed to be in condition for allowance, and such action is earnestly requested.

If any additional fee is required, please charge Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 5/23/06



Jordan M. Becker
Reg. No. 39,602

Customer No. 48102
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030
(408) 720-8300